Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A server comprising:

first means for categorizing permission setting values indicating whether object information items of various ~~attribute~~ attributes of a registered user are disclosable to other persons or not depending on a level of the disclosability; and

second means for managing the permission setting values ~~hierarchically~~ hierarchically,

wherein said second means checks, when there is a request from the user to change the permission setting value for any permission level other than the highest-level operation for any of the object information items, consistency of the permission setting value for each level higher than the level for which the change request has been made with the permission setting value for which the change request has been made,

said second means corrects, when there is contradiction in said consistency, the permission setting value for each level higher than the level for which the request to change the setting value has been made.

2. (original) A server according to claim 1, wherein

said first means categorizes said permission setting values into three respective levels for determining whether an open operation, a read operation, and a write operation are executable with respect to any of the object information items.

3. (original) A server according to claim 2, wherein

said second means manages said permission values so that executability of open operation is set as a permission level higher than said executability of read operation, and executability of read operation is set as a permission level higher than said executability of write operation, and

said second means includes detection means for detecting contradiction in a specified one of the permission setting values based on vertical relations among the permission levels.

4. – 5. (canceled)

6. (currently amended) A server according to ~~claim 4~~ claim 1, wherein

said second means manages said object information items by imparting vertical relations thereto in accordance with types of the object information items and systematically categorizing the object information items.

7. (canceled)

8. (currently amended) A server ~~according to claim 7, wherein,~~comprising:

first means for categorizing permission setting values indicating whether object information items of various attributes of a registered user are disclosable to other persons or not depending on a level of the disclosability; and

second means for managing the permission setting values hierarchically,

said second means checks, when there is a request from the user to change the permission setting value for an arbitrary one of the levels for any of the object information items, consistency of the permission setting value belonging to each of the object information items higher in rank than the object information item to which the setting value that has received the change request belongs with the setting value that has received the change request, and

said ~~detection~~ second means corrects, when there is contradiction in said consistency, the permission setting value belonging to any of the object information items higher in rank than the object information item to which the setting value that has received said change request belongs.

9. (original) A server according to claim 1, wherein

said second means manages said attribute information items by imparting vertical relations thereto in accordance with types of the attribute information items and systematically categorizing the attribute information items.

10. (currently amended) A server comprising:

an interface for receiving transmitted information;

storage ~~means; and~~ means;

means for reading information stored in the storage means therefrom, ~~wherein~~

wherein said storage means has an entry table for storing object information items corresponding to various attribute of a registered user and permission setting values indicating whether said attribute information items are disclosable to other persons or not, said permission setting values being categorized in accordance with a level of the disclosability ~~thereof~~thereof,

wherein said permission setting values are categorized into a plurality of levels having vertical relations thereamong;

wherein said entry table stores the setting value given to any of the plurality of levels,

means for extracting a request to change any of the permission setting values from received information;

judging means for judging whether or not the permission setting value for which said change request has been made is contradictory to any of the permission setting values higher in rank than the setting value by referencing said entry table; and

means for correcting, when there is contradiction between the setting value for which said change request has been made and any of the permission setting values higher in rank than the setting value, the higher rank permission setting value.

11. (cancel)

12. (currently amended) A server according to ~~claim 11~~ claim 10, wherein

said permission setting values are categorized into three respective levels for determining whether an open operation, a read operation, and a write operation are executable with respect to any of the object information items, and

said entry table stores the setting value given to any of said three levels.

13. – 14. (canceled)

15. (original) A server according to claim 11, further comprising:

an external storage device storing therein copy data of said entry table.

16. (currently amended) A method for controlling a server, comprising the ~~step~~ steps of:

categorizing permission setting values indicating whether object information items corresponding to various ~~attribute~~ attributes of a registered user are disclosable to other persons or not into a plurality of ~~levels; and~~ levels;

hierarchically managing said object information items by imparting thereto vertical relations depending on a level of the ~~disclosability~~ disclosability;

receiving, from said registered user, a request to change the permission setting value for a specified one of the object information items;

determining a level of the permission setting value for which the change request has been made;

judging whether there is contradiction between the permission setting value belonging to any level higher than the determined level and the permission setting value for which said change request has been made; and

correcting, when there is contradiction, the permission setting value belonging to the level higher than said determined level,

wherein said object information items are managed by imparting vertical relations thereto in accordance with types of the object information items and categorizing the object information items.

17. – 18. (canceled)

19. (currently amended) A method according to ~~claim 18~~ claim 16, further comprising the steps of:

receiving, from said registered user, a request to change the permission setting value for a specified one of the object information items;

determining a level to which the object information item belongs;

judging whether or not there is contradiction between the permission setting value for the object information item belonging to any level higher than the level of the object information item to which the permission setting value that has received the change request belongs and the permission setting value that has received the change request; and

notifying, when there is contradiction, the user that the setting change request has been refused.

20. – 24. (canceled)

25. (new) A server according to claim 1, wherein said object information items include identification information of a user terminal and communication capability information of said user terminal; and

wherein when there is a request from the user to change the permission setting value of said communication capability information from a not permitted state to a permitted state, said second means sets the permission setting value of said identification information to a permitted state, and when the permission setting value of said identification information is changed from a permitted state to a not permitted state, said second means sets the permission setting value of said communication capability to a not permitted state.